#4

35.G2331

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	
KAZUOMI OISHI	Examiner: NYA
	Group Art Unit: 3642
Application No.: 09/222,846	
Filed: December 30, 1998	
For: IMAGE INPUT APPARATUS, IMAGE INPUT METHOD, RECORDING MEDIUM, AND ENCRYPTION PROCESSING PROGRAM STORED IN COMPUTER-READABLE MEDIUM	February 24, 1999

Assistant Commissioner for Patents
Washington, D.C. 20231

CLAIM TO PRIORITY

Sir:

Applicant hereby claims priority under the International Convention and all rights to which he is entitled under 35 U.S.C. § 119 based upon the following Japanese Priority Application:

003367/1998 filed January 9, 1998

A certified copy of the priority document is enclosed.

Applicant's undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All

correspondence should continue to be directed to our address given below.

Respectfully submitted,

Jack M. Arnold

Attorney for Applicant

Registration No. 25,823

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

F502\A635296\mw

CFG2331 US
09/222,846
GAU 3642

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
事項と同一であることを証明する。
is is to certify that the annexed is a true copy of the following application as filed
his Office.

願年月日
of Application: １９９８年　１月　９日

願番号
cation Number: 平成１０年特許願第００３３６７号

願人
ant (s): キヤノン株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

１９９９年　１月２９日

特許庁長官
Commissioner,
Patent Office 伊佐山建志

出証番号　出証特平１１－３００２３８０

【書類名】　特許願
【整理番号】　3439018
【提出日】　平成10年 1月 9日
【あて先】　特許庁長官殿
【国際特許分類】　H04N 5/00
【発明の名称】　画像入力装置および方法並びに記憶媒体
【請求項の数】　21
【発明者】
【住所又は居所】　東京都大田区下丸子３丁目３０番２号　キヤノン株式会社内
【氏名】　大石　和臣
【特許出願人】
【識別番号】　000001007
【氏名又は名称】　キヤノン株式会社
【代理人】
【識別番号】　100090273
【弁理士】
【氏名又は名称】　國分　孝悦
【電話番号】　03-3590-8901
【手数料の表示】
【予納台帳番号】　035493
【納付金額】　21,000円
【提出物件の目録】
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　9705348
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　画像入力装置および方法並びに記憶媒体

【特許請求の範囲】

【請求項１】　画像信号をディジタル情報に変換する変換手段と、

暗号化鍵を用いて前記ディジタル情報を暗号化する暗号化手段と、

前記暗号化手段が前記ディジタル情報の暗号化を終了した後に前記暗号化鍵を消去する暗号化鍵消去手段とを有することを特徴とする画像入力装置。

【請求項２】　前記変換手段は前記ディジタル情報を高能率符号化する符号化手段を有し、前記暗号化手段は前記高能率符号化したディジタル情報を暗号化することを特徴とする請求項１に記載の画像入力装置。

【請求項３】　被写体を撮影して画像信号を生成する撮像手段を有し、前記変換手段は前記撮像手段により生成された画像信号をディジタル情報に変換することを特徴とする請求項１または２に記載の画像入力装置。

【請求項４】　前記暗号化鍵を外部から入力する暗号化鍵入力手段を具備することを特徴とする請求項１～３の何れか１項に記載の画像入力装置。

【請求項５】　前記暗号化鍵を内部で発生する暗号化鍵発生手段を具備することを特徴とする請求項１～３の何れか１項に記載の画像入力装置。

【請求項６】　前記暗号化鍵は共通鍵暗号化のための暗号化鍵であることを特徴とする請求項４または５に記載の画像入力装置。

【請求項７】　前記暗号化鍵発生手段で発生された内部暗号化鍵を外部から入力するインターフェースを具備し、前記インターフェースを介して暗号化された内部暗号化鍵を出力することを特徴とする請求項５に記載の画像入力装置。

【請求項８】　前記内部暗号化鍵は共通鍵暗号化のための暗号化鍵であり、前記外部暗号化鍵は公開鍵暗号化のための暗号化鍵であることを特徴とする請求項７に記載の画像入力装置。

【請求項９】　前記暗号化したディジタル情報を外部に出力する通信手段を具備することを特徴とする請求項１～８の何れか１項に記載の画像入力装置。

【請求項１０】　前記暗号化したディジタル情報を記録する記録手段を具備することを特徴とする請求項１～９の何れか１項に記載の画像入力装置。

【請求項１１】　画像信号をディジタル情報に変換する変換処理と、

暗号化鍵を用いて前記ディジタル情報を暗号化する暗号化処理と、

前記ディジタル情報の暗号化を終了した後に前記暗号化鍵を消去する暗号化鍵消去処理とを行うことを特徴とする画像入力方法。

【請求項１２】　前記ディジタル情報を高能率符号化し、前記高能率符号化されたディジタル情報を暗号化することを特徴とする請求項１１に記載の画像入力方法。

【請求項１３】　被写体を撮影する撮像処理により前記画像信号を生成することを特徴とする請求項１１または１２に記載の画像入力方法。

【請求項１４】　前記暗号化したディジタル情報を外部に出力する出力処理を行うことを特徴とする請求項１１～１３の何れか１項に記載の画像入力方法。

【請求項１５】　前記暗号化したディジタル情報を記録する記録処理を行うことを特徴とする請求項１１～１４の何れか１項に記載の画像入力方法。

【請求項１６】　請求項１～１０に記載の各手段としてコンピュータを機能させるためのプログラムを格納したことを特徴とする記憶媒体。

【請求項１７】　請求項１１～１５の何れか１項に記載の画像入力方法の手順をコンピュータに実行させるためのプログラムを格納したことを特徴とする記憶媒体。

【請求項１８】　画像信号をディジタル情報に変換する変換手段と、

前記ディジタル情報を暗号化する暗号化手段と、

前記暗号化手段が暗号化を行うための暗号化鍵を外部から入力する暗号化鍵入力手段とを有することを特徴とする画像入力装置。

【請求項１９】　画像信号をディジタル情報に変換する変換手段と、前記ディジタル情報を暗号化する暗号化手段とを有する画像入力装置に対して着脱自在であり、

前記暗号化手段が暗号化を行うため、および暗号化された前記ディジタル情報を復号するための鍵を記憶することを特徴とする記憶媒体。

【請求項２０】　画像信号をディジタル情報に変換する変換手段と、

前記ディジタル情報を内部暗号化鍵により暗号化する画像暗号化手段と、

前記内部暗号化鍵を暗号化する鍵暗号化手段と、

前記鍵暗号化手段が暗号化を行うための暗号化鍵を外部から入力する暗号化鍵入力手段とを有することを特徴とする画像入力装置。

【請求項２１】　画像信号をディジタル情報に変換する変換手段と、前記ディジタル情報を内部暗号化鍵により暗号化する画像暗号化手段と、前記内部暗号化鍵を暗号化する鍵暗号化手段とを有する画像入力装置に対して着脱自在であり、

前記鍵暗号化手段が暗号化を行うための暗号化鍵および暗号化された前記内部暗号化鍵を復号するための復号鍵を記憶することを特徴とする記憶媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、画像入力装置および方法並びに記憶媒体に関するものである。

【０００２】

【従来の技術】

スチル・カメラやビデオ・カメラ、あるいはスキャナ等のような画像入力装置は、被写体を撮影して得られた画像信号や、動画像や静止画像等の画像信号を入力し、画像情報として再生できるような形式に変換して出力したり、あるいは記録装置を用いて記憶媒体に記録したりするようにしている。

【０００３】

前記記憶媒体は、ある程度の長期間にわたって保存することが可能であるので、前記保存した画像情報を後で観賞したり、あるいは再利用したりするのに都合が良い。また、再生装置は、前記記憶媒体に記録された画像情報から人間にとって有意義な画像を形成し、プリンターやディスプレイ等の出力装置を用いて画像を再現する。

【０００４】

最近は、ディジタル技術の進展により、従来はアナログ方式で実現されていた前記画像入力装置等は、ディジタル方式のものに徐々に切り換えられつつある。これらのディジタル方式の画像入力装置は、ほとんどの場合、撮影対象あるいは

入力対象を光学的に捉え、それを光電変換して電気信号を生成し、次いでアナログ／ディジタル変換した後、所定の画像処理を施すようにしている。そして、その結果として形成される画像／画像情報を予め定められた形式のディジタル情報として出力する。

【０００５】

ここで、予め定められた形式とは、ＭＨ、ＭＲ、ＭＭＲ、Ｔ１ＦＦ、ＪＰＥＧ、ＭＰＥＧ等といった画像／画像情報に対する情報源符号化方式による符号のことを意味している。

【０００６】

そして、再生装置がその復号アルゴリズムを用いることにより、符号から復号して形成した情報をプリンターやディスプレイ等の出力装置に出力したときに、人間が画像／画像として理解できるような情報である。

【０００７】

以下では、前述の予め定められた形式のディジタル情報として出力される画像／画像情報を、情報源符号化された画像／画像情報と呼ぶ。情報源符号化された画像／画像情報、あるいはそれから復号された画像／画像情報を、例えばパーソナル・コンピュータのような情報処理装置に取り込み、その形式に対応した画像／画像情報編集処理ソフトウェアを用いて編集することは極めて容易である。

【０００８】

情報源符号化された画像／画像情報、あるいはそれを編集した情報を複製したときの画質は原本と全く同一である。従来のアナログ方式の場合には、編集や複製は画質の劣化を必ずもたらしていたために画像処理に制限が課されていたが、この点でディジタル方式は圧倒的な利便性の向上をもたらした。

【０００９】

ところで、従来のアナログ方式では複製を繰り返すことは必ず画質の劣化を伴ったがゆえに、違法な複製行為が行なわれるということはあってもそれが現実的に大きな問題となることは少なかった。したがって、そのような不正な複製行為を禁止する方法は特に設けられていなかった。

【００１０】

しかし、ディジタル方式では原本と全く同一の複製を無制眼に生成することが可能であるので、複製行為を誰でも自由に行なえるとすれば、著作物の観賞権利に対する対価を消費者が映画等の画像著作物の製作者等に対して払う必要は無くなるので、著作物の製作者等に対して大きな脅威となることは明らかである。

【００１１】

あるいは別の例として、例えば、著作物の原本となる画像／画像情報が情報源符号化された画像情報としてコンピュータに記録されている場合に、クラッカーがそのコンピュータにアクセスし、その画像／画像情報を不当に複製して、正規の著作物製品よりも安い価格で販売することや、その著作物を新たに編集して他の著作物として販売することも考えられる。

【００１２】

以上のような、ディジタル情報の複製の問題に対して、次に述べる暗号の技術を用いた対策が有効である。なお、暗号とは、情報の意味が当時者以外にはわからないように情報を変換することをいう。

【００１３】

暗号において、元の文を平文という。また、それを第三者には意味が分からない暗号文に変えることを暗号化といい、その変換手順を暗号アルゴリズムという。平文、暗号文といってもテキストに限るわけではなく、データ、音声、画像などあらゆる情報を想定している。

【００１４】

暗号化は、暗号化鍵というパラメータに依存する変換である。当事者が暗号文を元の平文に戻すことを復号といい、暗号化鍵に対応するパラメータ（復号鍵と呼ぶ）を用いて行なう。

【００１５】

また、当事者以外の第三者が暗号文を元の平文に戻すこと、あるいは復号鍵を見いだすことを解読という。現代の暗号では、暗号の安全性を暗号あるいは復号に用いる鍵に帰着させており、鍵を知らなければたとえ暗号アルゴリズムを知っていても平文は得られないように作られている。したがって、暗号器の作成者でも解読はできない。

【００１６】

暗号には多くのアルゴリズムがあるが、以下では暗号化鍵を公開できるか否かの観点から、非対称暗号（公開鍵暗号）と対称暗号（慣用暗号）の二つに分類する。

【００１７】

非対称暗号は公開鍵暗号とも呼ばれ、暗号化鍵と復号鍵が異なり、暗号化鍵から復号鍵が容易に計算できないようになっており、暗号化鍵を公開鍵といい、復号鍵を秘密に保持して使われる暗号のことをいう。

【００１８】

非対称暗号は、以下の特徴を持っている。

（１）暗号化鍵と復号鍵とが異なり暗号化鍵を公開できるため、暗号化鍵を秘密に配送する必要がなく、鍵配送が容易である。

（２）各利用者の暗号化鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよい。

（３）送られてきた通信文の送信者が偽物でないこと、及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。暗号機能と認証機能を実現できる非対称暗号として、ＲＳＡ暗号（R. L. Rivest, A. Shamir and L. Adleman, “A method of obtaining digital signatures and public key cryptosytems,” Comm of ACM,）がある。

【００１９】

また、この他に、エルガマル暗号（T. E. ElGamal, “A public key cryptosystem and a signature scheme based on discretre logarithms,” IEEE Transaction on Information Theory, Vol. IT-31, No. 4, pp-469－472, 1985）が有名である。

【００２０】

認証機能のみを実現できる非対称暗号として、Ｆｉａｔ－Ｓｈａｍｉｒ暗号（A. Ｆｉａｔ, A. Ｓｈａｍｉｒ, “Ｈｏｗ ｔｏ ｐｒｏｖｅ ｙｏｕｒｓｅｌｆ：ｐｒａｃｔｉｃａｌ ｓｏｌｕｔｉｏｎｓ ｏｆ ｉｄｃｎｔｉｆｉｃａｔｉｏｎ ａｎｄ ｓｉｇｎａｔｕｒｅ ｐｒｏｂｌｅｍｓ,”, Ｐｒｏｃ. ｏｆ ＣＲＹＰＴＯ’８６, １９８７）や、Ｓｃｈｎｏｒｒ暗号（C. Ｐ. Ｓｃｈｎｏｒｒ, “Ｅｍｃｉｅｎｔ ｓｉｇｎａｔｕｒｅ ｇｅｎｅｒａｔｉｏｎ ｂｙ ｓｍａｒｔ ｃａｒｄｓ,” Ｊｏｕｒｎａｌ ｏｆ Ｃｒｙｐｔｏｌｇｙ ｖｏｌ ４, ｐｐ. １６１－１７４, １９９１）が有名である。

【００２１】

対称暗号は、暗号化鍵と復号鍵が同一の暗号であり、共通鍵暗号とも呼ばれている。１９７９年代後半に公開鍵暗号が現れて、従来から存在する対称暗号は慣用暗号とも呼ばれるようになった。

【００２２】

対称暗号は、適当な長さの文字列（ブロック）ごとに同じ鍵で暗号化するブロック暗号と、文字列またはビットごとに鍵を変えていくストリーム暗号に分けることができる。

【００２３】

ブロック暗号には、文字の順序を置き換えて暗号化する転置式暗号や、文字を他の文字に換える換字式暗号等があり、アルゴリズムが公開されているＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）や、ＦＥＡＬ（Ｆａｓｔ ｄａｔａ Ｅｎｃｉｐｈｅｒｍｅｎｔ ＡＬｇｏｒｉｔｈｍ）といった暗号が商用暗号として広く用いられている。

【００２４】

ストリーム暗号は、メッセージに乱数をＸＯＲ（排他論理和）して、内容を撹乱する方式であり、無限周期の乱数列を１回限りの使い捨て鍵として用いるバーナム暗号が有名である。

【００２５】

以上の暗号の技術を用いて、コンピュータ等に記録される画像／画像情報等に対して暗号化を施し、復号鍵を安全に保管しておけば、暗号文、つまり画像／画

像情報を暗号化した情報が盗まれて複製されたとしても、画像／画像情報そのものが盗まれたことにはならないので被害を被ることはない。つまり、前述のような複製の問題を解決できると考えられる。

【００２６】

ところが、従来は画像／画像情報等がコンピュータ等に出力されてからコンピュータ上で暗号化が実行されていたので、画像入力装置から画像／画像情報が出力されてからコンピュータ上で暗号化されるまでの間は情報源符号化された画像／画像情報として存在し、その間に画像／画像情報を盗まれてしまうという問題があった。

【００２７】

この問題に対して、画像入力装置内部で暗号化を行なう対処法がある。このとき、暗号化される前の画像／画像情報が外部に取り出されることが無いように暗号化機能を組み込む必要がある。

【００２８】

このような手段としては、その内部に格納してあるプログラムやデータを取り出すことが物理的に困難になるように暗号化部をＩＣチップ化することや、さらには、ＩＣチップ化した暗号化部の内部にセンサーを設けておき、ＩＣチップ内部のデータを取り出そうとする物理的動作を検出したときにその内部のプログラムやデータを消去・破壊するといったものが考えられる。このような外部からの攻撃に対する耐性をタンパー・レジスタンス（Ｔａｍｐｅｒ　Ｒｅｓｉｓｔａｎｃｅ）と呼ぶ。

【００２９】

【発明が解決しようとする課題】

タンパー・レジスタンスを有する暗号化部を組み込んだ画像入力装置では、その強度を弱めないために、固定の値が暗号化鍵としてあらかじめ装置に記録されており、その値は容易に変更できないことが普通である。

【００３０】

一つの装置に一つの鍵が割り当てられている場合、複数のユーザがそれを共有して使う時にはそれらのユーザー間では暗号化（秘匿）機能は無いに等しいこと

になってしまう。

【００３１】

一方、複数の鍵をあらかじめ用意しておき、ユーザ毎に別々の鍵を用いるという方法もあるが、この時は装置内部の暗号化部のメモリ量が増え、コストの上昇につながる問題が生じる。

【００３２】

いずれにせよ、不特定多数のユーザに対して個別に対応できないという問題があった。さらに、これらのタンパー・レジスタンスを有する装置や媒体は、その性質を永遠に有するとは限らず、新しい攻撃手段によりその性質が容易に無効化される恐れもあった。

【００３３】

本発明は前述の問題点にかんがみ、情報入力装置のタンパー・レジスタンスに依存することなく安全性を保つことができるようにすることを目的とする。

【００３４】

【課題を解決するための手段】

本発明の画像入力装置は、画像信号をディジタル情報に変換する変換手段と、暗号化鍵を用いて前記ディジタル情報を暗号化する暗号化手段と、前記暗号化手段が前記ディジタル情報の暗号化を終了した後に前記暗号化鍵を消去する暗号化鍵消去手段とを有することを特徴としている。

【００３５】

また、本発明の画像入力装置の他の特徴とするところは、前記変換手段は前記ディジタル情報を高能率符号化する符号化手段を有し、前記暗号化手段は前記高能率符号化したディジタル情報を暗号化することを特徴としている。

【００３６】

また、本発明の画像入力装置のその他の特徴とするところは、被写体を撮影して画像信号を生成する撮像手段を有し、前記変換手段は前記撮像手段により生成された画像信号をディジタル情報に変換することを特徴としている。

【００３７】

また、本発明の画像入力装置のその他の特徴とするところは、前記暗号化鍵を

外部から入力する暗号化鍵入力手段を具備することを特徴としている。

【００３８】

また、本発明の画像入力装置のその他の特徴とするところは、前記暗号化鍵を内部で発生する暗号化鍵発生手段を具備することを特徴としている。

【００３９】

また、本発明の画像入力装置のその他の特徴とするところは、前記暗号化鍵は共通鍵暗号化のための暗号化鍵であることを特徴としている。

【００４０】

また、本発明の画像入力装置のその他の特徴とするところは、前記暗号化鍵発生手段で発生された内部暗号化鍵を外部から入力するインターフェースを具備し、前記インターフェースを介して暗号化された内部暗号化鍵を出力することを特徴としている。

【００４１】

また、本発明の画像入力装置のその他の特徴とするところは、前記内部暗号化鍵は共通鍵暗号化のための暗号化鍵であり、前記外部暗号化鍵は公開鍵暗号化のための暗号化鍵であることを特徴としている。

【００４２】

また、本発明の画像入力装置のその他の特徴とするところは、前記暗号化したディジタル情報を外部に出力する通信手段を具備することを特徴としている。

【００４３】

また、本発明の画像入力装置のその他の特徴とするところは、前記暗号化したディジタル情報を記録する記録手段を具備することを特徴としている。

【００４４】

本発明の画像入力方法は、画像信号をディジタル情報に変換する変換処理と、暗号化鍵を用いて前記ディジタル情報を暗号化する暗号化処理と、前記ディジタル情報の暗号化を終了した後に前記暗号化鍵を消去する暗号化鍵消去処理とを行うことを特徴としている。

【００４５】

また、本発明の画像入力方法の他の特徴とするところは、前記ディジタル情報

を高能率符号化し、前記高能率符号化されたディジタル情報を暗号化することを特徴としている。

【００４６】

また、本発明の画像入力方法のその他の特徴とするところは、被写体を撮影する撮像処理により前記画像信号を生成することを特徴としている。

【００４７】

また、本発明の画像入力方法のその他の特徴とするところは、前記暗号化したディジタル情報を外部に出力する出力処理を行うことを特徴としている。

【００４８】

また、本発明の画像入力方法のその他の特徴とするところは、前記暗号化したディジタル情報を記録する記録処理を行うことを特徴としている。

【００４９】

また、本発明の記憶媒体は、前記各手段としてコンピュータを機能させるためのプログラムを格納したことを特徴としている。

【００５０】

また、本発明の記憶媒体の他の特徴とするところは、前記画像入力方法の手順をコンピュータに実行させるためのプログラムを格納したことを特徴としている。

【００５１】

また、本発明の画像入力装置のその他の特徴とするところは、画像信号をディジタル情報に変換する変換手段と、前記ディジタル情報を暗号化する暗号化手段と、前記暗号化手段が暗号化を行うための暗号化鍵を外部から入力する暗号化鍵入力手段とを有することを特徴としている。

【００５２】

また、本発明の記憶媒体のその他の特徴とするところは、画像信号をディジタル情報に変換する変換手段と、前記ディジタル情報を暗号化する暗号化手段とを有する画像入力装置に対して着脱自在であり、前記暗号化手段が暗号化を行うため、および暗号化された前記ディジタル情報を復号するための鍵を記憶することを特徴としている。

【００５３】

また、本発明の画像入力装置のその他の特徴とするところは、画像信号をディジタル情報に変換する変換手段と、前記ディジタル情報を内部暗号化鍵により暗号化する画像暗号化手段と、前記内部暗号化鍵を暗号化する鍵暗号化手段と、前記鍵暗号化手段が暗号化を行うための暗号化鍵を外部から入力する暗号化鍵入力手段とを有することを特徴としている。

【００５４】

また、本発明の記憶媒体のその他の特徴とするところは、画像信号をディジタル情報に変換する変換手段と、前記ディジタル情報を内部暗号化鍵により暗号化する画像暗号化手段と、前記内部暗号化鍵を暗号化する鍵暗号化手段とを有する画像入力装置に対して着脱自在であり、前記鍵暗号化手段が暗号化を行うための暗号化鍵および暗号化された前記内部暗号化鍵を復号するための復号鍵を記憶することを特徴としている。

【００５５】

本発明は前記技術手段よりなるので、暗号化鍵は暗号化終了後には情報入力装置から消去され、これにより、暗号化された情報を復号するための暗号化鍵（復号鍵）を第三者が得ることができなくなり、情報入力装置のタンパー・レジスタンスに依存することなく安全性を保つことが可能となる。

【００５６】

また、本発明の他の特徴によれば、外部とのインターフェイスを利用して暗号化鍵（復号鍵）を入力するので、不特定多数のユーザに対応することができ、人間の操作の手間を省くことができるようになるとともに、暗号化鍵が第三者に盗まれる恐れを少なくすることができるようになる。

【００５７】

【発明の実施の形態】

（第１の実施の形態）

次に、図１を参考に本発明の画像入力装置および方法並びに記憶媒体の第１の実施の形態を説明する。

【００５８】

図１は、本実施の形態の画像入力装置の概略を示すブロック図であり、１は撮像装置、２は中央情報処理装置（ＣＰＵ）、３は制御プログラム用メモリ、４は作業用メモリ、５は暗号化器であり、これはタンパー・レジスタンスを持つように封止一体化されたモジュール１０となっていることを示している。

【００５９】

本実施の形態の画像入力装置においては、読みとる対象を撮像装置１により撮像してアナログの画像信号を生成し、これをディジタル画像信号に変換するディジタル変換処理を施すようにしている。

【００６０】

前記撮像装置１は、制御プログラム用メモリ３に格納されているプログラムによって良い画像が得られるように制御され、その結果として画像データを出力するように動作する。

【００６１】

次に、この画像データは、ＣＰＵ２において画像処理等を施された後、情報源符号化（高能率符号化）された画像／画像情報に変換されて、暗号化器５に入力される。

暗号化器５は、外部インターフェイス７から入力される暗号化鍵をパラメータとして、入力に対する暗号化をその内部で実行して暗号文を生成して出力する。出力された暗号化された画像データは不図示の記憶媒体に記憶される。外部インターフェイス７は、暗号化鍵を装置外部から受け取ったり、あるいは装置内から暗号化鍵を出力するために使われたりするインターフェイスである。

【００６２】

前記の構成において、タンパー・レジスタンスの特徴により、撮像装置１と、ＣＰＵ２と、制御プログラム用メモリ３と、作業用メモリ４と、暗号化器５の内部に存在するデータや通信内容を外部から得ることはできない。

【００６３】

次に、暗号化に用いる暗号方式、暗号化鍵の指定方法の組合せについて説明する。用いる暗号方式は、公開鍵暗号と共通鍵暗号の２つの場合がある。共通鍵暗号を用いる場合は、暗号化鍵を他者に知られないように指定する必要がある。こ

れに対して公開鍵暗号を用いる場合は、暗号化鍵は公開可能であるので必ずしも他者に知られないように指定する必要はない。

【００６４】

暗号化鍵の指定方法は、以下のような方法がある。すなわち、第１の方法は装置を製造する時に制御プログラム用メモリ３に記憶させておく方法である。

また、第２の方法は、操作スイッチ８から入力する方法であり、第３の方法は、外部インターフェイス７から入力する方法である。

【００６５】

第１の方法は、さらに、装置の一つ一つに異なった鍵を記憶させておく場合と、ある種類の装置の全てに共通の鍵を記憶させておく場合とに分けられる。しかし、いずれの場合にせよその装置を使う正規の者だけが暗号化鍵に対応する復号鍵を知るように運用しなければならず、その運用は現実的には困難が伴うことがある。

【００６６】

第２の方法は、装置の使用者自身が自分しか知らない暗号化鍵を装置に直接入力できるので、他の者が暗号化鍵を知る恐れは少なく、第１の方法よりも安全性が向上する利点を有している。しかし、人間が扱いやすい鍵を自由に定められるとは限らないので、人間が記憶したり入力するのに困難な大きさや内容の鍵の場合には、その操作は煩わしいものとなることがある。

【００６７】

第３の方法は、外部インターフェイス７に適当な外部装置を接続して、その外部装置から画像入力装置に暗号鍵を入力する方法である。この方法を採用する場合、鍵を入力するための通信が外部装置と画像入力装置との間で自動的に行なわれるようにすれば、人間の手間は軽減される。

【００６８】

次に、外部インターフェイス７に接続される外部装置としてＩＣカードを採用した場合について説明する。画像入力装置のユーザは、ある程度の記憶能力と計算能力を持つＩＣカードを携帯し、その中にはそのユーザだけが知っている暗号化鍵と対応する復号鍵が記憶されるとする。

【００６９】

ＩＣカードを分解してその暗号化鍵を得ることは極めて困難になるように製造できると考えられる。ユーザが画像入力装置を使用する時に、自分のＩＣカードを外部インターフェイス７に接続する。画像入力装置は、撮影した画像をＩＣカードから入力される暗号鍵で暗号化して出力し、入力された暗号化鍵を暗号化終了後に消去する。

【００７０】

このようにすると、暗号化された画像情報は、対応する復号鍵を持つそのユーザだけが復号できることになる。ユーザは、操作時に自分のＩＣカードを外部インターフェイスに接続して撮影操作を行なうだけでよいので、操作上の負担は第２の方法よりは少ない。

【００７１】

暗号化方式として公開鍵暗号あるいは共通鍵暗号を単独に利用する場合と、それらを組み合わせる場合がある。いずれの方法で暗号化鍵を指定して暗号化したとしても、その暗号文は対応する復号鍵を用いて復号することができ、情報源符号化された画像情報を得ることが可能である。

【００７２】

一例として、共通鍵暗号を単独に用いる場合について述べる。図１に示したように、外部装置としてＩＣカード２０を用いる。前記ＩＣカード２０には共通鍵暗号の暗号鍵生成手段と、暗号化鍵を画像入力装置に入力するための通信手段が設けられているといる。

【００７３】

暗号化鍵は、例えば、乱数を発生させることにより生成され、その実行は容易であるものとする。ユーザがＩＣカード２０を外部インターフェイス７を介して画像入力装置に接続し、撮影操作を行なう。外部インターフェイス７に接続されたＩＣカード２０は、通信手段を介して、生成した暗号化鍵を画像入力装置に送信する。

【００７４】

画像入力装置は、入力された暗号化鍵を用いて撮影した画像を暗号化器５によ

り暗号化して出力する。そして、この暗号を生成するために用いられた暗号化鍵は、暗号化を終了した後で画像入力装置のメモリから消去される。ユーザはＩＣカード２０を情報処理装置に接続すると、情報処理装置はＩＣカード２０から読みだした暗号化鍵を用いて、画像入力装置から出力された画像を復号することができる。

【００７５】

なお、以上に説明した画像入力装置としては、スキャナやスチル・カメラ、ビデオ・カメラ等が考えられる。他に、複写機やファクシミリにも本発明を適用することが可能である。さらに、キーボード、マウス、ペン・タブレット、センサー、タッチ・パネル等のような、任意の情報入力装置に関して、本発明を適用できることは明らかである。

【００７６】

（第２の実施の形態）

次に、暗号化方式として公開鍵暗号と共通鍵暗号を組み合わせる場合について説明する。外部装置としてＩＣカードを用い、ＩＣカードには公開鍵暗号の暗号化鍵生成手段と、画像入力装置との通信手段が配設されているとする。画像入力装置には、乱数発生手段と公開鍵暗号化手段と共通鍵暗号化手段が内蔵されているものとする。

【００７７】

ユーザがＩＣカードを画像入力装置に接続し、撮影操作を行なう。接続されたＩＣカードは公開鍵暗号の暗号化鍵（以下では、公開鍵と呼ぶ）を画像入力装置に通信する。

【００７８】

画像入力装置は、乱数発生器に設けられている乱数発生手段を用いて共通鍵暗号化のための暗号化鍵を生成し、撮影した画像をその生成した暗号化鍵を用いて内蔵の共通鍵暗号化手段により暗号化して出力する。

【００７９】

それと同時に、その共通鍵暗号化のための暗号化鍵を、入力された公開鍵を用いて公開鍵暗号化手段で暗号化して出力する。共通鍵暗号化のための暗号化鍵は

暗号化終了後に画像入力装置のメモリから消去される。

【００８０】

ユーザはＩＣカードを情報処理装置に接続し、画像入力装置から出力された公開鍵暗号で暗号化された共通鍵暗号化のための暗号化鍵を、ＩＣカードに格納されている公開鍵に対応する秘密鍵で復号し、共通鍵暗号化のために使われた暗号化鍵を得る。そして、その暗号化鍵を用いて、画像入力装置から出力された暗号化画像を復号する。

【００８１】

図２は、図１の中央情報処理装置２、制御プログラム用メモリ３、作業用メモリ４からなるコンピュータシステムにより構成される各手段を説明する機能ブロック図である。

【００８２】

図２に示したように、本実施の形態の画像入力装置１００は、撮像手段１０１と、変換手段１０２と、符号化手段１０３と、暗号化手段１０４と、暗号化鍵消去手段１０５と、通信手段１０７と、記録手段１０８と、暗号化鍵形成手段１０９とを有している。

【００８３】

前記撮像手段１０１は、被写体を撮影して画像信号を生成するものであり、変換手段１０２は、前記画像信号をディジタル情報に変換するためのものである。

【００８４】

また、符号化手段１０３は、前記ディジタル情報を高能率符号化するものであり、暗号化手段１０４は前記符号化したディジタル情報を暗号化するためのものである。

【００８５】

暗号化鍵形成手段１０９は、前記暗号化手段が暗号化を行うための暗号化鍵を発生もしくは外部から入力するためのものであり、暗号化鍵消去手段１０５は前記暗号化手段がディジタル情報の暗号化を終了した後に前記暗号化鍵を消去するものである。

【００８６】

通信手段１０７は、前記暗号化したディジタル情報を外部に出力するものであり、記録手段１０８は前記暗号化したディジタル情報を記憶媒体に記録するものである。

【００８７】

次に、前述のように構成された画像入力装置の画像入力方法を図３のフローチャートを参照しながら説明する。

図３に示したように、本実施の形態の画像入力装置１００は、最初のステップＳ１において、被写体を撮像手段１０１で撮影して画像信号を生成する。

【００８８】

次に、ステップＳ２に進み、前記画像信号をディジタル情報に変換する変換処理を変換手段１０２により行う。

その後、ステップＳ３に進み、符号化手段１０３によって前記ディジタル情報を高能率符号化する。

【００８９】

次に、ステップＳ４に進み、前記符号化されたディジタル情報を暗号化するための暗号化鍵を暗号化鍵形成手段１０９にて発生もしくは外部から入力する暗号化鍵形成処理を行う。

次に、ステップＳ５に進み、前記符号化されたディジタル情報を前記暗号化鍵を用いて暗号化手段１０４で暗号化する。

【００９０】

次に、ステップＳ６に進み、前記ディジタル情報の暗号化を終了した後に前記暗号化鍵を暗号化鍵消去手段１０５によって消去する暗号化鍵消去処理を行う。

【００９１】

以上説明したように、本実施の形態の画像入力方法によれば、暗号化鍵は暗号化終了後には消去されるので、暗号化された情報を復号するための暗号化鍵（復号鍵）を第三者が得ることができなくなる。

【００９２】

したがって、本実施の形態の画像入力装置の場合には、情報入力装置のタンパー・レジスタンスに依存することなく安全性を保つことができる。しかも、外部

インターフェイス７を利用して暗号化鍵（復号鍵）を情報入力装置に入力することにより、不特定多数のユーザに対応することができるようになる。

【００９３】

これにより、人間の操作の手間を省き、暗号化鍵を第三者に盗まれる恐れを少なくすることができ、かつメモリ量を増やすこと無しに、利便性と安全性を同時に向上させることができる。

【００９４】

（本発明の他の実施形態）

本発明は複数の機器（例えば、ホストコンピュータ、インタフェース機器、リーダ、プリンタ等）から構成されるシステムに適用しても１つの機器からなる装置に適用しても良い。

【００９５】

また、前述した実施形態の機能を実現するように各種のデバイスを動作させるように、前記各種デバイスと接続された装置あるいはシステム内のコンピュータに対し、前記実施形態の機能を実現するためのソフトウェアのプログラムコードを供給し、そのシステムあるいは装置のコンピュータ（ＣＰＵあるいはＭＰＵ）に格納されたプログラムに従って前記各種デバイスを動作させることによって実施したものも、本発明の範疇に含まれる。

【００９６】

また、この場合、前記ソフトウェアのプログラムコード自体が前述した実施形態の機能を実現することになり、そのプログラムコード自体、およびそのプログラムコードをコンピュータに供給するための手段、例えばかかるプログラムコードを格納した記憶媒体は本発明を構成する。かかるプログラムコードを記憶する記憶媒体としては、例えばフロッピーディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００９７】

また、コンピュータが供給されたプログラムコードを実行することにより、前述の実施形態の機能が実現されるだけでなく、そのプログラムコードがコンピュ

ータにおいて稼働しているＯＳ（オペレーティングシステム）あるいは他のアプリケーションソフト等の共同して前述の実施形態の機能が実現される場合にもかかるプログラムコードは本発明の実施形態に含まれることは言うまでもない。

【００９８】

さらに、供給されたプログラムコードがコンピュータの機能拡張ボードやコンピュータに接続された機能拡張ユニットに備わるメモリに格納された後、そのプログラムコードの指示に基づいてその機能拡張ボードや機能拡張ユニットに備わるＣＰＵ等が実際の処理の一部または全部を行い、その処理によって前述した実施形態の機能が実現される場合にも本発明に含まれることは言うまでもない。

【００９９】

【発明の効果】

以上説明したように、本出願の発明によれば、暗号化終了後には情報入力装置から暗号化鍵を消去するようにしたので、暗号化された情報を復号するための暗号化鍵（復号鍵）を第三者が得られないようにすることができる。これにより、情報入力装置のタンパー・レジスタンスに依存することなく高い安全性を保つことができる。

【０１００】

また、本発明の他の特徴によれば、外部とのインターフェイスを利用して暗号化鍵（復号鍵）を情報入力装置に入力するようにしたので、不特定多数のユーザに対応することができ、人間の操作の手間を省き、暗号化鍵を第三者に盗まれる恐れを少なくすることができ、かつメモリ量を増やすこと無しに、利便性と安全性を同時に向上させることができる。

【図面の簡単な説明】

【図１】

本発明の実施の形態に係る暗号化機能付き画像入力装置の構成を示すブロック図である。

【図２】

本発明の実施の形態に係る暗号化機能付き画像入力装置の機能構成を示す機能ブロック図である。

【図３】

本発明の画像入力方法の一例を示すフローチャートである。

【符号の説明】

１　撮像装置

２　ＣＰＵ

３　制御プログラム用メモリ

４　作業用メモリ

５　暗号化器

６　機械的動作部

７　外部インターフェイス

８　操作スイッチ

１００　画像入力装置

１０１　撮像手段

１０２　変換手段

１０３　符号化手段

１０４　暗号化手段

１０５　暗号化鍵消去手段

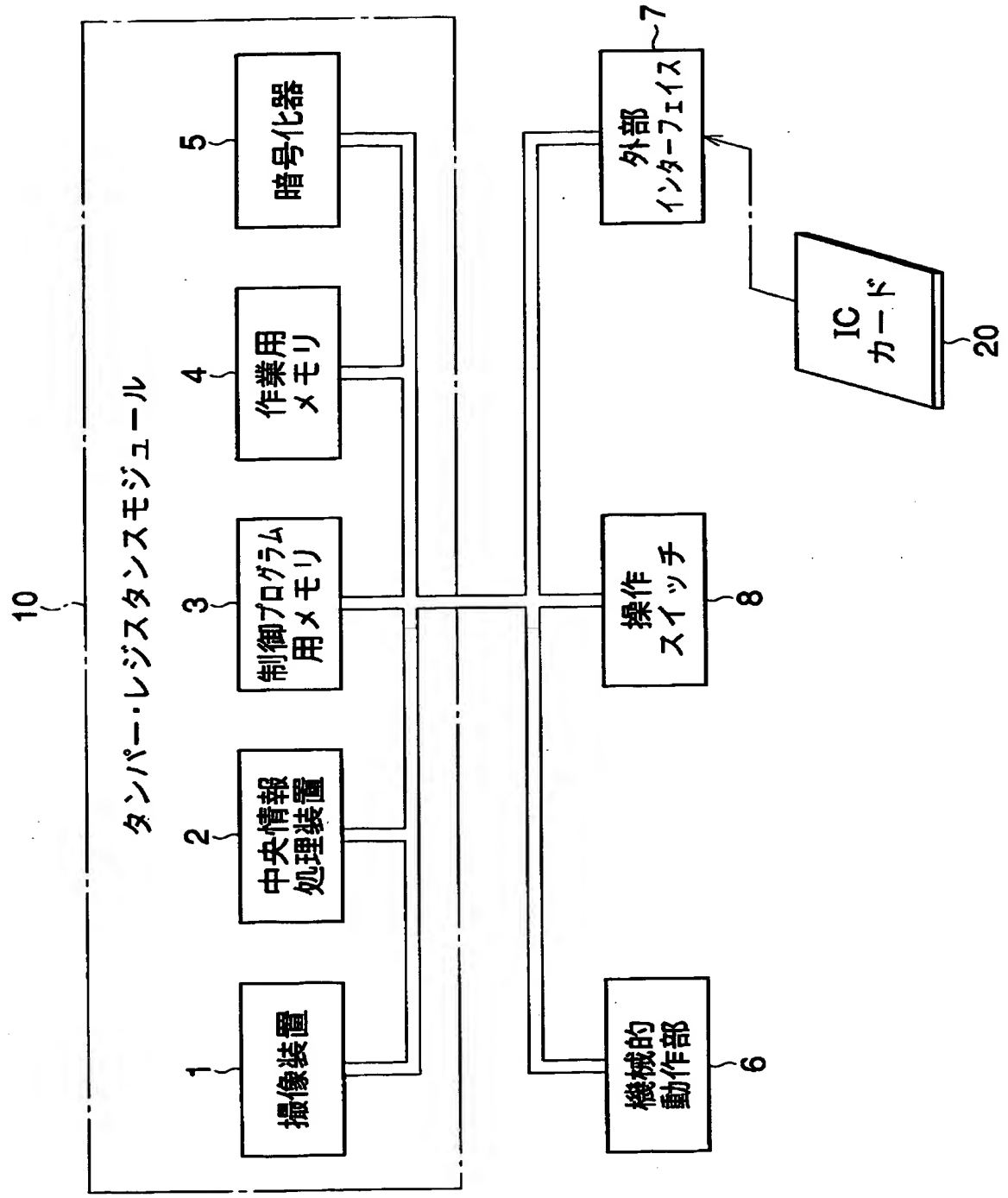
１０７　通信手段

１０８　記録手段

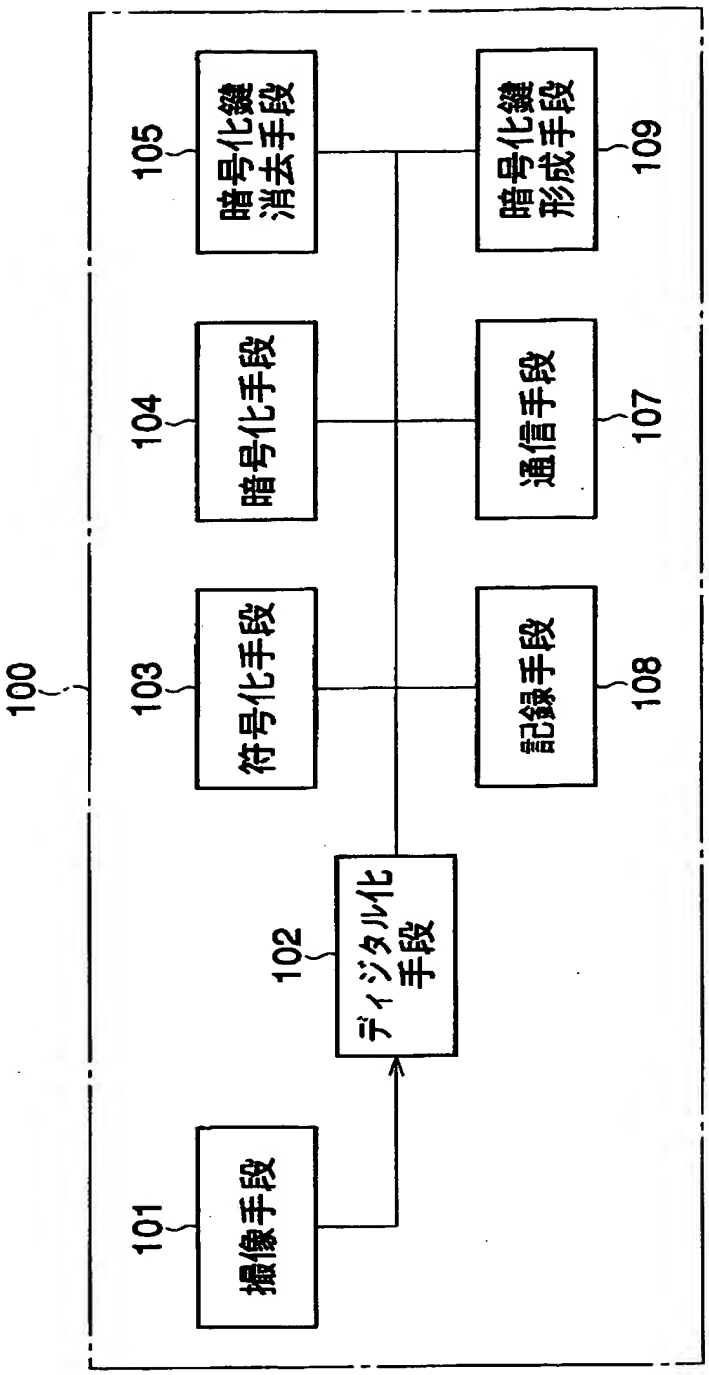
１０９　暗号化鍵形成手段

【書類名】　図面

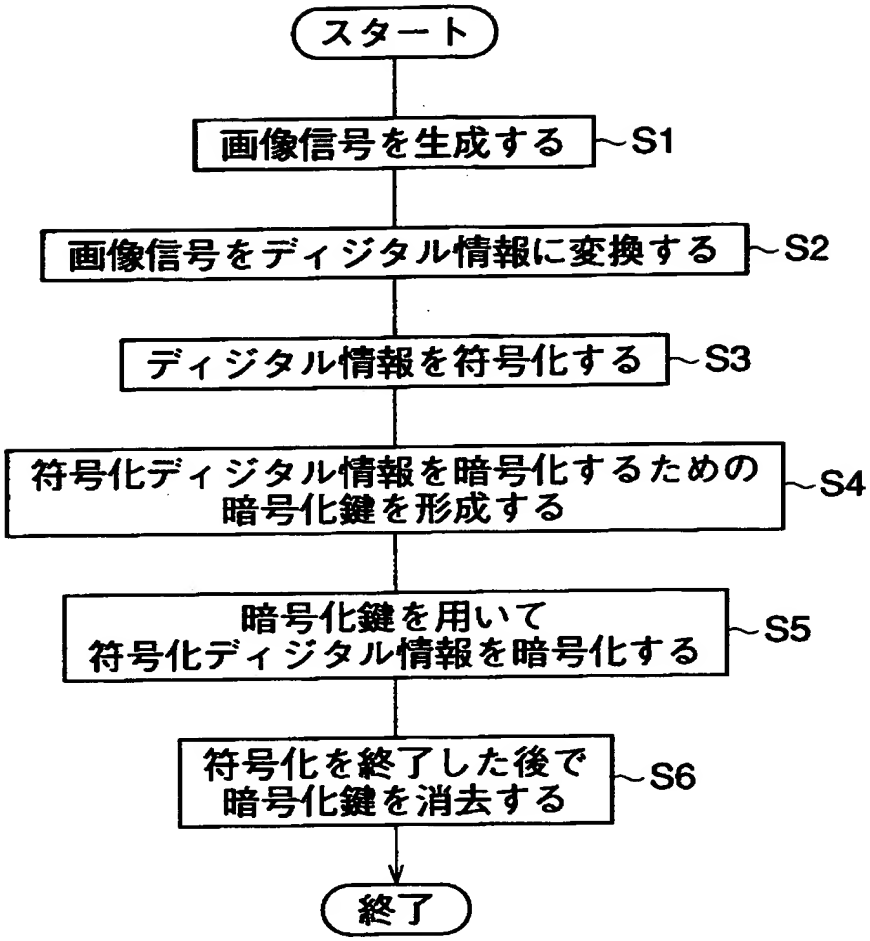
【図１】


タンパー・レジスタンスモジュール
10
撮像装置
1
中央情報処理装置
2
制御プログラム用メモリ
3
作業用メモリ
4
暗号化器
5
機械的動作部
6
外部インターフェイス
7
操作スイッチ
8
ICカード
20

【図２】


100
101
撮像手段
102
ディジタル化手段
103
符号化手段
104
暗号化手段
105
暗号化鍵消去手段
107
通信手段
108
記録手段
109
暗号化鍵形成手段

【図３】


スタート
画像信号を生成する
S1
画像信号をディジタル情報に変換する
S2
ディジタル情報を符号化する
S3
符号化ディジタル情報を暗号化するための
暗号化鍵を形成する
S4
暗号化鍵を用いて
符号化ディジタル情報を暗号化する
S5
符号化を終了した後で
暗号化鍵を消去する
S6
終了

【書類名】　　要約書

【要約】

【課題】　情報入力装置のタンパー・レジスタンスに依存することなく高い安全性を保つことができるようにする。

【解決手段】　画像信号をディジタル情報に変換する変換手段１０２と、前記ディジタル情報を暗号化する暗号化手段１０４と、前記暗号化手段１０４が暗号化を行うための暗号化鍵を外部から入力する暗号化鍵入力手段１０９と、前記暗号化手段１０４がディジタル情報の暗号化を終了した後に前記暗号化鍵を消去する暗号化鍵消去手段１０５とを設け、暗号化された情報を復号するための暗号化鍵（復号鍵）を第三者が得られないようにする。

【選択図】　　図２

【書類名】　職権訂正データ
【訂正書類】　特許願

＜認定情報・付加情報＞
【特許出願人】
【識別番号】　000001007
【住所又は居所】　東京都大田区下丸子３丁目３０番２号
【氏名又は名称】　キヤノン株式会社
【代理人】　申請人
【識別番号】　100090273
【住所又は居所】　東京都豊島区東池袋１丁目１７番８号　池袋ＴＧホーメストビル５階　國分特許事務所
【氏名又は名称】　國分　孝悦

出　願　人　履　歴　情　報

識別番号　　〔０００００１００７〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　東京都大田区下丸子３丁目３０番２号
氏　名　キヤノン株式会社